REMARKS

Reconsideration of this application, as amended, is respectfully requested.

The Examiner is thanked for conducting a telephone interview on January 11, 2006.

THE CLAIMS

Independent claims 1, 6 and 12 have been amended to clarify the feature of the present invention whereby the contents data is copyrighted electronic contents data, as supported by the disclosure in the specification at, for example, page 2, lines 15-19.

In addition, independent claims 1, 6 and 12 have been amended to explicitly recite that the server receives from the user terminal contents specifying data specifying the copyrighted electronic contents data to be distributed, and that the first key is generated at the server from contents information relating to the copyrighted electronic contents data to be distributed.

No new matter has been added, and it is respectfully requested that the amendments to claims 1, 6 and 8 be approved and entered.

THE PRIOR ART REJECTION

Claims 1, 2 and 4-12 were rejected under 35 USC 102 as being anticipated by USP 6,539,364 ("Moribatake et al"). This rejection, however, is respectfully traversed.

First, it is respectfully submitted that Moribatake et al relates to issuing, receiving and spending electronic cash, and does not at all disclose, teach or suggest encrypting and decrypting copyrighted electronic contents data as recited in amended independent claims 1, 6 and 8. In addition, it is respectfully submitted that Moribatake et al does not disclose, teach or even remotely suggest first and second keys having features as recited in independent claims 1, 6 and 8. And still further, it is respectfully submitted that the disparate portions of Moribatake et al that were cited by the Examiner cannot logically be integrated to disclose a functional encryption and decryption technique as recited in independent claims 1, 6 and 8.

According to the present invention as recited in amended independent claims 1, 6 and 8, copyrighted electronic contents data is encrypted and decrypted to be distributed from a server to a user terminal through a network. According to the present invention as recited in the amended independent claims, contents specifying data, which specifies the copyrighted electronic contents data to be distributed, is received from the user terminal. A first key is generated at the server from contents information relating to the copyrighted electronic contents data to be distributed. A second key is generated at the server from: a variable parameter received from the user terminal, a H/W key ID retrieved from a user information database by using a user ID received from the user terminal, and the first key, and then the generated second key is sent to the user terminal. At the user terminal, the first key is decrypted from the variable parameter, the H/W key ID, and the second key. At the server, moreover, the (copyrighted electronic) contents data to be distributed is encrypted by using the first key, and the encrypted contents data is sent to the user terminal. Finally, the encrypted contents data at the user terminal by using the decrypted first key.

That is, according to the present invention as recited in amended independent claims 1, 6 and 8, the contents data to be distributed which is encrypted and decrypted using the first key is copyrighted electronic contents data, and the first key is generated from contents information relating to the copyrighted electronic contents data to be distributed.

According to dependent claims 10-12, moreover, the contents information of the contents data comprises a size of the contents data and a preceding update date of the contents data.

It is respectfully pointed out that Moribatake et al, by contrast, relates to obtaining electronic cash and using the obtained electronic cash to purchase items, using signatures transmitted between a user, a trustee equipment, a bank, an electronic cash issuer, and a store. According to Moribatake et al, the electronic cash is distributed by, for example, issuing a "signature" from an issuer to a user in which the signature is prepared based on a public user key, a cash amount and a secret key of the issuer of the electronic cash (i.e. signature SKI(PKU,x) of Moribatake et al).

It is respectfully submitted that the electronic cash of Moribatake et al clearly does not at all relate to copyrighted electronic contents data that is encrypted and decrypted to be distributed over a network.

It is respectfully submitted, moreover, that Moribatake et al clearly does not disclose, teach or suggest a first key which is used to encrypt and decrypt contents data and which is generated from contents information relating to the copyrighted electronic contents data to be distributed, or a second key which is generated from: a variable parameter received from the user terminal, a H/W key ID retrieved from a user information database by using a user ID received from the user terminal, and the first key, wherein the user terminal uses the variable parameter, the H/W key ID, and the second key to decrypt the first key.

The Examiner has cited disclosure from the first through fourth embodiments of Moribatake et al as relating to the claimed present invention. These embodiments disclose many keys that are used to encrypt and decrypt data. In particular, the trustee equipment 500, which in some embodiments registers and issues a license to the user equipment 300, generates secret key SKR and public key PKR. The user equipment 300 of Moribatake et al generates a secret key SKU and a public key PKU, and in at least the third and fourth embodiments, also generates a common key K. The issuer equipment 100 of Moribatake et al generates secret key SKI and public key PKI. And in at least the second embodiment of Moribatake et al, the bank equipment 200 stores pre-generated secret key SKBx for a cash amount x, and public bank key PKBx for cash amount x that is sent to issuer and user equipment 100 and 300.

The keys of Moribatake et al mentioned above are used to perform various encryption, decryption and authentication operations. However, Moribatake et al does not disclose, teach or suggest how any of the keys SKR, PKR, SKU, PKU, K, SKI, PKI, SKBx and PKBx are generated.

Since Moribatake et al does not disclose how the keys are generated or upon what data the generation of the keys is based, (except, possibly, for the disclosure that keys SKBx and PKBx are "for electronic cash x"), it is respectfully submitted that Moribatake et al cannot even remotely be considered to disclose a first key that is generated from contents information relating to the copyrighted electronic contents data to be distributed, or a second key which is generated from: a variable parameter received from the user terminal, a H/W key ID retrieved from a user information database by using a user ID received from the user terminal, and the first key.

Although it is not clear what features of Moribatake et al the Examiner considers to correspond to the keys of the claimed present invention, the Examiner may believe that the "signatures" disclosed by Moribatake et al correspond to the first and/or second key of the claimed present invention.

It is respectfully pointed out, however, that according to the claimed present invention the first key is used to encrypt data at the server, and the second key is used (along with the variable parameter and H/W key ID) to decrypt the first key.

And it is respectfully pointed out that the signatures disclosed by Moribatake et al are neither used to encrypt or decrypt information. By contrast, the signatures of Moribatake et al are formed by encrypting key(s) and other information, and the signatures themselves may be encrypted by still further keys. However, the signatures of Moribatake et al are not themselves used to encrypt or decrypt information. That is, the signatures of Moribatake et al are not keys. Thus, it is respectfully submitted that the signatures of Moribatake et al also do not correspond to the first and second keys of the claimed present invention.

In more detail, according to the first embodiment of Moribatake et al, the user equipment 300 is registered by sending a public user key PKU (which is generated at the user equipment with key generating device 330) and a user name IdU to the trustee equipment 500. The trustee equipment 500 stores PKU and IdU and generates a signature (or "license") SKR(PKU) based on PKU, using the secret trustee equipment key SKR. The user equipment 300 then authenticates the received signature SKR(PKU) by using the public trustee equipment key PKR. See column 4, lines 11-39.

Thus, although the Examiner has cited column 4, lines 16-17 as disclosing generating a first key in the manner of independent claims 1, 6 and 8, it is clear that the "user registration procedure" of Moribatake et al does not include a description of how keys SKR, PKR, PKU and SKU are generated, and clearly does not disclose, teach or suggest generating a first key from contents information relating to the copyrighted electronic contents data to be distributed, as according to the present invention as recited in amended independent claims 1, 6 and 8.

In order to issue cash to a user according to the first embodiment of Moribatake et al, the user sends the key PKU, the ID data IdU, and a requested electronic cash amount x to the issuer 100 as a withdrawal request. The issuer 100 performs some accounting processing and then creates a signature SKI(PKU, x) using the secret issuer key SKI and the public key PKU and cash amount x. The signature SKI(PKU, x) is sent to the user equipment 300, which authenticate the signature with the public issuer key PKI. If the signature is verified, then the user equipment 300 updates its electronic cash balance to reflect the addition of cash amount x. See column 4, line 40 to column 5, line 6, for example, of Moribatake et al.

Thus, the disclosure of issuing cash according to the first embodiment of Moribatake et al does not disclose how keys SKI and PKI are generated. In addition, it should be clear that the signature SKI(PKU, x) is not a key but rather is a signature transmitted to indicate that the cash amount x is issued to the user. Therefore, even though the cash amount x is variable and inputted by a user, the cash amount x is not used to create a key. That is, the cash amount x is not a variable parameter received from the user terminal and used to generate a second key.

The Examiner has also cited portions of the disclosure of the second embodiment (namely, column 7, lines 18-31 and column 7, line 66 to column 8, line 3) with respect to the generation of the second key.

It should be noted, however, that column 7, lines 18-31 of Moribatake et al (which the Examiner cited as disclosing the generation of the second key based on a H/W key ID) <u>discloses the same "user registration procedure" as the first embodiment procedure described at column 4, lines 11-39</u>. And it is respectfully submitted that just as the description of a "user registration procedure" of Moribatake et al does not disclose how a first key is generated, it also does not even remotely disclose the generation of a second key.

Indeed, even though the user registration procedure mentions a user name IdU, Moribatake et al does not disclose, teach or suggest looking up a H/W key ID from a database using the data IdU, and Moribatake et al does not disclose, teach or suggest that any of the keys SKR, PKR, SKU and PKU are generated based on a H/W key ID or any other information obtained using data IdU. Alternatively, if the Examiner is suggesting that key PKU corresponds to the H/W key ID of the claimed present invention, it is respectfully pointed out that PKU is not retrieved from a database using a user ID. It should be clear, moreover, from the description at column 4, lines 11-39 and column 7, lines 18-31 that license SKR(PKU) is not a key that is used to encrypt information, but rather is a license that is used to authenticate a user at by shop 400 as described at, for example, column 5, lines 41-46 of Moribatake et al.

According to the second embodiment of Moribatake et al, moreover, a bank equipment 200 is provided that issues a coupon for electronic cash to the user, which transmits the coupon to the issuer 100 together with the public user key PKU and cash amount x. The coupon SKBx(PKU) is generated at the bank using a secret key for cash amount x SKBx and is generated without knowledge at the bank 200 of the public user key PKU due to a "blinding" procedure performed on the public key PKU before it is transmitted from the user 300 to the bank 200.

The Examiner contends that column 7, line 66 to column 8, line 3 of Moribatake et al discloses transmitting the second key to the user terminal. It is respectfully pointed out, however, that the cited portion of Moribatake et al discloses sending data from the user equipment 300 to the issuer 100. In addition, the coupon (signature) SKBx(PKU) is not a key.

The Examiner has also cited elements of the third and fourth embodiments of Moribatake et al as corresponding to the features of the claimed present invention. In particular, the Examiner contends that the encrypting and decrypting of data according to the claimed present invention is disclosed in the third and fourth embodiments of Moribatake et al. It is respectfully submitted, however, that Moribatake et al does not disclose the first and second keys of the claimed present invention, as explained hereinabove. And it is respectfully submitted that the third and fourth embodiments of Moribatake et al are no more relevant to the claimed present invention than the first and second embodiments.

The third embodiment of Moribatake et al, moreover, discloses a technique in which there is no trustee equipment 500 and in which communication between the user equipment 300 and issuer 100 is conducted through the bank 200, so that the bank relays information between the user and issuer. In order to conceal data from the bank, another key, common key K, is used. The common key K is encrypted, together with public key PKU, using the public issuer key PKI and is sent to the issuer 100 via the bank 200. The issuer decrypts PKI(PKU, K) to obtain K, which it then uses to encrypt the license SKI(PKU) as K(SKI(PKU)) that is sent to the user 300 through the bank 200. The user decrypts the encrypted license using common key K and verifies license SKI(PKU) using public issuer key PKI. See column 9, line 51 to column 10, line 55 of Moribatake et al.

It should be noted that although Moribatake et al refers to PKI(PKU, K) as an encrypted key, the unit "PKI(PKU, K)" is not actually used to encrypt any data. Rather, the common key K, which is used to encrypt data, is encrypted within PKI(PKU, K). It should also be noted that the license SKI(PKU) is a license for identifying/authenticating the user at the shop 400, in a similar manner to license SKR(PKU) described above with respect to the first embodiment.

The fourth embodiment of Moribatake et al, moreover, is very similar to the third embodiment, except that key identification data KID is created at the issuer 100 when the common key is obtained from PKI(PKU, K) so as to index the common key K in a database. With this structure, it is not necessary for the user to re-transmit the common key K when requesting the issuer to issue cash, since the issuer will already have key K on file from when the license SKI(PKU) was issued. And with this structure, the withdrawal request from the user to the issuer can then be concealed from the bank by encryption with common key K. See, for example, column 12, line 41 to column 14, line 23.

Thus, as recognized by the Examiner, the third and fourth embodiments of Moribatake et al do disclose sending encrypted data (i.e. the encrypted license K(SKI(PKU))) from the issuer to the user.

However, the encrypted content is merely a license such as SKI(PKU), or a signature verifying electronic cash issuance when making a withdrawal. The common key K, moreover, must correspond to the first key in the Examiner's interpretation of the third and fourth embodiments of Moribatake et al, since it is the common key K that is used to encrypt the license SKI(PKU). However, the common key K is generated at the user equipment 300.

Therefore, the common key K is not generated at the server (from contents information relating to the copyrighted electronic contents data to be distributed) and is not decrypted at the user terminal, as according to the present invention as recited in claims 1, 6 and 8 with respect to the first key.

Finally, it is respectfully submitted that the various disparate citations from Moribatake et al clearly cannot logically be considered to form a coherent encryption and decryption technique in the manner of the claimed present invention.

In particular, the Examiner has cited portions of Moribatake et al related to the trustee 500, the issuer 100 and the bank 200 as relating to the server of the claimed present invention. However, according to Moribatake et al these various components are separate, perform different functions, and in some embodiments, take steps to conceal information from other ones of the components. (See for example the concealment of information from the bank described above with respect to the second, third and fourth embodiments.) It is respectfully submitted, therefore, that the combination of citations relating to these different components of Moribatake et al is simply not logical.

Still further, it is also respectfully pointed out that the Examiner has even cited conflicting passages of Moribatake et al with respect to the same feature of the present invention. For example, at the top of page 3 the Examiner asserts that a first key is disclosed at column 4, lines 16-17 and column 13, lines 2-4. However, the first citation relates to trustee keys SKR, PKR, while the second citation relates to issuer keys SKI, PKI. In addition, also on page 3 of the Office Action the Examiner cites column 9, lines 61-63, column 10, lines 38-39, column 12, lines 52-54 and column 13, lines 40-41 with respect to encrypting and decrypting data with the first key. These cited portions, however, relate to encryption performed with the common key K. Thus, on page 3 of the Office Action and within the rejection of claim 1 the Examiner has identified three different possibilities for the "first key" according to the present invention.

It is again respectfully submitted that the disparate citations from the various embodiments of Moribatake et al cannot reasonably be combined into a single, functional encryption/ decryption method that corresponds to the claimed present invention.

In view of the foregoing, it is respectfully submitted that the present invention as recited in amended independent claims 1, 6 and 8, as well as claims 2, 4, 5, 7 and 9-12 respectively depending therefrom, clearly patentably distinguishes over Moribatake et al, under 35 USC 102 as well as under 35 USC 103.

* *

Entry of this Amendment, allowance of the claims and the passing of this application to issue are respectfully solicited.

If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned for prompt action.

Respectfully submitted,

Douglas Holtz
Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.
220 Fifth Avenue - 16th Floor
New York, New York 10001-7708
Tel. No. (212) 319-4900
Fax No. (212) 319-5101
DH:iv
encs.